WHAT IS CLAIMED IS:

1. An individually usable memory device, connectable to a host device, for performing mutual authentification between a server device and the memory device by use of a passcode, comprising:

an interface adapted to receive time information from said host device;

a non-volatile memory for storing pass-information which is related to pass-information of said server device and which is defined for each user; and

a processing device which, in response to a request from said host device, generates said passcode from the pass-information in said non-volatile memory and a time information from said host device, and which transmits said passcode to said host device through said interface without sending said pass-information to said host device.

2. The memory device according to claim 1, wherein the memory device is configured such that a success-time of the mutual authentification between said memory device and said server device via said host device is stored in said non-volatile memory, so that it is impossible to illegally alter the stored success-time afterwards, and whether or not the memory device may be used is controlled on the basis of said success-time that cannot be illegally altered.

3. The memory device according to claim 2, wherein:

said processing device includes a time examination unit for verifying the time information from said host device;

said time examination unit stores the time information when an initial time verification is successful; and

said processing device causes generation of said passcode to be failed when the time information from said host device is not later than the success time of said connection authentification, and causes generation of said passcode to be failed or said passcode to be deleted when the time information from said host device is later than an expiration date of said pass-information, so that the passcode to be transmitted to said host device may be limited to the predetermined number of bytes.

4. The memory device according to claim 2, wherein

said processing device encrypts license data that can be used for protection of a copy right after the mutual authentification with either said host device or said server device, stores the license date in said non-volatile memory, stores said pass-information in said non-volatile memory as license data, and with reading-out of the license data being prohibited afterwards, makes it possible to use the license data for the generation of said passcode.

5. The memory device according to claim 2, wherein:

said non-volatile memory holds license data with an

expiration date; and

said processing device compares the expiration date of said license data with said success-time when said license data is accessed, and stops the access to the license data with said expiration date or delete said license data when the expiration date is not later than said success time.

6. A single chip microcomputer that is mounted on an individually usable memory device, connectable to a host device, for performing mutual authentification between a server device and the memory device by use of a passcode, comprising:

receiving means adapted for receiving a time information from said host device;

reading-out means for reading out from a non-volatile memory in said memory device a pass-information which is related to a pass-information of said server device and which is defined for each user for said memory device;

generating means for generating said passcode on the basis of said pass-information and time information from said host device; and

transmittance means for transmitting said passcode to said host device through an interface within said memory device without transmitting said pass-information to said host device.

7. The single chip microcomputer according to claim 6,

wherein a success-time of the mutual authentification between said memory device and said server device via said host device is written into said non-volatile memory, said memory device is configured such that said success-time stored cannot be illegally altered afterwards, and whether or not the memory device can be used is controlled on the basis of said success-time that cannot be illegally altered.

8. A passcode generator, connectable to a first computer used by a user, which generates a passcode for authenticating the user with a second computer capable of communicating with said first computer, comprising:

an interface connected to said first computer;

a memory for storing pass-information agreeing with pass-information stored in said second computer and a user ID of said user;

a time examination unit for, time information being stored therein or in said memory, comparing time information from said first computer with the time information stored therein or in said memory when receiving the time information from said first computer, and updating the time information stored therein or in said memory to the time information from said first computer when the time information from said first computer is later than the time information stored therein or in said memory; and

a random number generator for generating said passcode

on the basis of the pass-information in said memory and the time information stored therein or in said memory, and sending said passcode and said user ID to said first computer through said interface when the time information from said first computer is later than the time information stored therein or in said memory.

9. The passcode generator according to claim 8, wherein said random number generator sends error information in place of said passcode to said first computer through said interface when the time information from said first computer is not later than the time information stored therein or in said memory.

10. The passcode generator according to claim 8, wherein

said memory stores a password; and

said time examination unit, when the time information from said first computer is not later than the time information stored therein or in said memory, compares the password from said first computer with the password in said memory, and if the password from said first computer agrees with the password in said memory, updates the time information stored therein or in said memory to the time information from said first computer.

11. The passcode generator according to claim 8, wherein

said memory stores data with an expiration date therein; and

said passcode generator includes a data supervising

unit for verifying said expiration date using the time information stored therein or in said memory which were updated, when the time information from said first computer is later than the time information in said memory.

12. The passcode generator according to claim 11, wherein,

said memory stores encrypted content data therein;

said data with an expiration date is a license for decrypting said content data; and

said data supervising unit receives said data with an expiration date sent from said second computer through said first computer and said interface when said second computer is successful in user authentification using said passcode and stores said received data with an expiration date.

13. The passcode generator according to claim 11, wherein

said memory stores a password therein;

said data supervising unit makes said data with an expiration date invalid when the time information from said first computer is not later than the time information stored therein or in said memory, and makes said invalidated data with an expiration date valid when the password from said first computer is compared with the password in said memory and the password from said first computer agrees with the password in said memory.

14. The passcode generator according to claim 13, wherein said password is a password given to a administrator different from said user.

15. The passcode generator according to claim 8, wherein,

said time examination unit stores the number of updates of time information stored therein or in said memory and sends error information in place of said passcode to said first computer through said interface when said number of updates exceeds a predetermined number of update times within a predetermined period of time.

16. A passcode generator, connectable to a first computer used by a user, which generates a passcode for authenticating the user with a second computer capable of communicating with said first computer, comprising:

an interface connected to said first computer;

a memory for storing pass-information agreeing with the pass-information stored in said second computer and a user ID of said user;

a time examination unit for, time information stored therein or in said memory, sending the time information stored therein or in said memory to said first computer, receiving the time information in said first computer from said first computer when said first computer judges that the time information in said first computer is later than the time

information stored therein or in said memory, and updating the time information stored therein or in said memory to the time information from said first computer; and

a random number generator for generating said passcode on the basis of the pass-information in said memory and said time information and sending said passcode and said user ID to said first computer through said interface when the time information in said first computer is later than the time information stored therein or in said memory.